Altiris™ Patch Management Solution for Linux® 7.1 SP2 from Symantec™ User Guide

Symantec™

Altiris™ Patch Management Solution for Linux® 7.1 SP2 from Symantec™ User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec, the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

See "*Altiris™ Patch Management Solution for Linux 7.1 SP2 from Symantec™ Third-Party Legal Notices*" on page 67.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Managed Services	Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Education Services	Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about enterprise services, please visit our web site at the following URL:

www.symantec.com/business/services/

Select your country or language from the site index.

Contents

Chapter 1

Introducing Patch Management Solution for Linux

This chapter includes the following topics:

About Patch Management Solution for Linux

Patch Management Solution for Linux ensures that your Red Hat Linux and SUSE Linux computers have the most up-to-date patches applied and protected against security threats. The solution lets you inventory the managed Linux computers for security vulnerabilities and then reports on the findings. It provides you with the tools that let you download and distribute the needed software updates. Patch Management Solution for Linux lets you set up an automatic update schedule to ensure that managed computers are up-to-date and protected on an on-going basis.

See "Platforms supported by Patch Management Solution for Linux" on page 20.

See "Implementing Patch Management Solution for Linux" on page 15.

What's new in Patch Management Solution for Linux 7.1 SP2

In the 7.1 SP2 release of Patch Management Solution for Linux, the following new features are introduced:

- Support for Red Hat Enterprise Linux 6.0 and 6.1, all variants
- Support for SUSE Linux Enterprise Server and SUSE Linux Enterprise Desktop version 11 SP1
- Performance and reliability improvements

See "About Patch Management Solution for Linux" on page 11.

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-1 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-1 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-2 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Implementing Patch Management Solution for Linux

This chapter includes the following topics:

Implementing Patch Management Solution for Linux

Patch Management Solution for Linux requires some components to be configured or enabled before others to function correctly. The recommended workflow is as follows:

See "About Patch Management Solution for Linux" on page 11.

Table 2-1 Process for implementing Patch Management Solution for Linux

Step	Action	Description
Step 1	Install or upgrade the solution.	Use Symantec Installation Manager to install the solution. See "About installing Patch Management Solution" on page 20. See "About upgrading Patch Management Solution for Linux" on page 21.

Table 2-1 Process for implementing Patch Management Solution for Linux *(continued)*

Step	Action	Description
Step 2	Install or upgrade the Symantec Management Agent.	Install or upgrade the Symantec Management Agent for UNIX, Linux, and Mac on every computer to which you want to send patches. For more information, see topics about installing or upgrading the Symantec Management Agent in the *Symantec Management Platform User Guide*. See "Where to get more information" on page 12.
Step 3	Install or upgrade the software update plug-in.	Install the plug-in that manages all of the Patch Management Solution for Linux functionality on a client computer. See "Installing the software update plug-in" on page 23. See "Upgrading the software update plug-in" on page 24.
Step 4	Configure the Patch Management Solution core settings.	(Optional) Configure the software update files storage location settings. See "Configuring patch management Core Services settings" on page 27.
Step 5	Type the credentials.	Type the Novell Mirror Credentials and Red Hat Network account credentials. See "Configuring Linux remediation settings" on page 29.
Step 6	Configure the software updates installation settings.	Configure when do you want to perform software update installation. See "Configuring software updates installation settings" on page 29.
Step 7	Configure the system assessment scan interval.	Configure when to run the system assessment scan, which inventories managed computers for the software updates that they require. See "Configuring the system assessment scan interval " on page 30.
Step 8	Download the Linux software updates metadata.	Download the Novell announcements and Red Hat errata metadata. Configure the metadata update schedule. See "Downloading the software updates catalog" on page 38.

Table 2-2 Process for installing software updates

Step	Action	Description
Step 1	Review and distribute available software updates.	View which software errata or announcements you need to install, then download updates and create software update policies. See "Downloading software updates" on page 44. See "Downloading and distributing software updates" on page 46.
Step 2	Evaluate the results.	Evaluate the results by running the **Software Update Delivery Summary** report and revisiting compliance reports. See "Viewing the software update delivery summary report" on page 47. See "Viewing Patch Management Solution reports" on page 58.

Chapter 3

Installing Patch Management Solution for Linux

This chapter includes the following topics:

System requirements for Patch Management Solution

Patch Management Solution requires the following:

- Symantec Management Platform 7.1 SP2

For details on Symantec Management Platform implementation, see the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

When you install or upgrade Patch Management Solution through the Symantec Installation Manager, Symantec Management Platform is installed automatically.

See "About installing Patch Management Solution" on page 20.

Platforms supported by Patch Management Solution for Linux

The Patch Management Solution for Linux component of Patch Management Solution supports the following operating systems:

- SUSE Linux Enterprise Server 10, 10 SP1-SP4, x86, x86_64
- SUSE Linux Enterprise Server 11, 11 SP1, x86, x86_64
- SUSE Linux Enterprise Desktop 10, 10 SP1-SP4, x86, x86_64
- SUSE Linux Enterprise Desktop 11, 11 SP1, x86, x86_64
- Red Hat Enterprise Linux AS/WS/ES 4 x86, x86_64
- Red Hat Enterprise Linux Server/Desktop 5 x86, x86_64
- Red Hat Enterprise Linux Server/Workstation/Client 6.0, 6.1, x86, x86_64

See "About Patch Management Solution for Linux" on page 11.

About installing Patch Management Solution

Starting from version 7.1, the Patch Management Solution installation includes the following components:

- Patch Management Solution for Windows
- Patch Management Solution for Linux
- Patch Management Solution for Mac

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For details on Symantec Management Platform implementation, see the *IT Management Suite 7.1 SP2 Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See "About Patch Management Solution for Linux" on page 11.

About upgrading Patch Management Solution for Linux

You upgrade this product from 7.1 or later to 7.1 SP2 by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information about migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at: http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at: http://www.symantec.com/docs/DOC4743

After you upgrade the solution, you must upgrade the Symantec Management Agent and the software update plug-in that are installed on the managed computers.

For more information about upgrading the Symantec Management Agent, see *Symantec Management Platform User Guide*.

See "Upgrading the software update plug-in" on page 24.

See "About Patch Management Solution for Linux" on page 11.

About uninstalling Patch Management Solution

Use the Symantec Installation Manager to uninstall this product.

See "About Patch Management Solution for Linux" on page 11.

About licensing Patch Management Solution

Each Symantec product comes with a seven-day trial license that is installed by default. You can register and obtain a 30-day evaluation license through the Symantec Web site at http://www.symantec.com/business/products/activating/ or purchase a full product license.

Use the Symantec Installation Manager to install licenses.

See "About Patch Management Solution for Linux" on page 11.

Chapter 4

Installing the Software Update Plug-in

This chapter includes the following topics:

About the software update plug-in

The software update plug-in manages patch management functionality on a client computer. When a client computer requires a certain software update, the update is sent from the Notification Server computer to the software update plug-in. The software update plug-in ensures that the update is applicable and not already installed, and then installs it.

See "Installing the software update plug-in" on page 23.

Installing the software update plug-in

The software update plug-in manages all of the Patch Management Solution functionality on a client computer.

See "About the software update plug-in" on page 23.

Note: If you have a large number of computers on which to install the software update plug-in, consider deploying it during off-peak hours to minimize network traffic. Deploying the software update plug-in can take some time, depending on the number of managed computers and the Symantec Management Agent settings.

See "Implementing Patch Management Solution for Linux" on page 15.

To install the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Software Update Plug-in Install**.
3. (Optional) In the right pane, make any wanted changes.

   For help, press F1 or click **Help > Context**.
4. Turn on the policy.
5. Click **Save changes**.

Upgrading the software update plug-in

If you upgraded Patch Management Solution from a previous version, you must also upgrade the Symantec Management Agent and the software update plug-ins that are installed on the target computers.

For more information about upgrading the Symantec Management Agent, see *Symantec Management Platform User Guide*.

See "About the software update plug-in" on page 23.

See "Implementing Patch Management Solution for Linux" on page 15.

To upgrade the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Software Update Plug-in Upgrade**.
3. (Optional) In the right pane, make any wanted changes.

   For help, press F1 or click **Help > Context**.
4. Turn on the policy.
5. Click **Save changes**.

Uninstalling the software update plug-in

You can uninstall the software update plug-in if there is an extended period of time when you do not want to use the patch management features on a managed computer and you want to eliminate any overhead that is caused by the plug-in.

See "About the software update plug-in" on page 23.

Ensure that the **Software Update Plug-in Install** policy is turned off before uninstalling the software update plug-in.

See "Installing the software update plug-in" on page 23.

To uninstall the software update plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, click **Software > Patch Management > Software Update Plug-in Uninstall**.
3. (Optional) In the right pane, make any wanted changes.

   For help, press F1 or click **Help > Context**.
4. Turn on the policy.
5. Click **Save changes**.

Chapter 5

Configuring Patch Management Solution for Linux

This chapter includes the following topics:

Configuring patch management Core Services settings

On the **Core Services** page you can configure to which location the software updates should be downloaded. You can also create custom severity levels that you can later apply to software updates.

The settings that you configure on the **Core Services** page apply to Windows and Linux components of Patch Management Solution.

See "About Patch Management Solution for Linux" on page 11.

To configure patch management Core Services settings

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management > Core Services**.
3. In the right pane, make any wanted changes.

   See "Core Services page" on page 30.
4. Click **Save Changes**.

Creating and assigning custom severity levels

Errata or announcements deemed critical may not necessarily be critical in your environment. You can create your own custom severity levels and assign them to errata and patches.

You first create custom severity levels, and then assign them to bulletins. You can alter custom severity levels. You cannot alter the vendor-specified severity levels.

See "About errata and patches" on page 43.

To create a custom severity level

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, click **Software > Patch Management > Core Services**.
3. In the right pane, click the **Custom Severity** tab.
4. In the **Severity Level** box, type the name that you want to give the custom severity level. For example, "Install right away!"
5. Click **Add**.
6. Click **Move Up** or **Move Down** to position custom severity levels in the list.
7. Click **Save Changes**.

To assign a custom severity level to a software bulletin

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. On the **Patch Remediation Center** page, in the software bulletin list, right-click a software bulletin, and then click **Custom Severity**.

3 Click a severity level.

4 Click **Refresh** to view the new data in the **Custom Severity** column.

Configuring Linux remediation settings

You can set up how you want Linux software updates distributed. You can configure package distribution and program settings.

See "About errata and patches" on page 43.

See "Implementing Patch Management Solution for Linux" on page 15.

To configure remediation settings

1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.

2 In the left pane, click **Software > Patch Management**.

3 Do one of the following:

- Click **Novell Settings > Novell Patch Remediation Settings**.
- Click **Red Hat Settings > Red Hat Patch Remediation Settings**.

4 In the right pane, make any wanted changes.

See "Linux patch remediation settings pages" on page 31.

5 Click **Save changes**.

Configuring software updates installation settings

You can configure when the software update plug-in installs the software updates and when to restart the target computer.

See "About the software update plug-in" on page 23.

See "Implementing Patch Management Solution for Linux" on page 15.

To configure the software updates installation settings

1 In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.

2 In the left pane, click **Software > Patch Management > Linux > Default Software Update Plug-in Settings**.

3 In the right pane, configure when and how you want to install updates.

See "Default Software Update Plug-in Settings page" on page 34.

4 Click **Save changes**.

Configuring the system assessment scan interval

The system assessment scan lets you periodically inventory operating systems, applications, and installed patches on managed computers with the software update plug-in installed. System assessment information is then used to determine which software updates the managed computer requires. Based on this information, filters are automatically created to assist with the targeting of software update policies.

You can configure how often you want to run the system assessment scan.

See "Implementing Patch Management Solution for Linux" on page 15.

To configure the system assessment scan interval

1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.

2 In the left pane, click **Software > Patch Management > Linux System Assessment Scan**.

3 In the right pane, under **Schedule**, configure how often to perform the system assessment scan on the managed computers and report it back to Notification Server.

4 Do not change the targeted filter from **Linux Computers with Software Update Plug-in Installed Target** unless you have a specific reason to do so.

5 Click **Save changes**.

Core Services page

The **Core Services** page lets you configure to which location the software updates should be downloaded. You can also create the custom severity levels that you later apply to software updates.

The settings that are defined on this page apply to Windows and Linux components of Patch Management Solution.

Only users with the **Patch Management Administrators** role can modify the settings on this page.

See "About errata and patches" on page 43.

See "Configuring patch management Core Services settings" on page 27.

See "Creating and assigning custom severity levels" on page 28.

Table 5-1 Options on the **Core Services** page

Option	Description
To Location	Specifies the location to which you want to download the software update packages. The default location is C:\Program Files\Altiris\Patch Management\Packages\Updates. If you change the location and you want to relocate existing software update packages, use the **Check Software Update Package Integrity** task. See "Relocating or checking the integrity of software update packages" on page 39.
Download from staging location	(Patch Management Solution for Windows only) Specifies the location to download packages from if you want to download them from a cache in a different location. For this functionality to work, the file structure in that location must be exactly the same as the folder structure under C:\Program Files\Altiris\Patch Management\Packages\Updates.
Severity Level	Lets you create a custom severity level that you can then assign to a bulletin.

Linux patch remediation settings pages

The **Novell Patch Remediation Settings** and **Red Hat Patch Remediation Settings** pages let you set up how you want Linux software updates distributed.

See "Configuring Linux remediation settings" on page 29.

Some of these settings are used as default values in the **Distribute Software Updates** wizard.

All new Linux software updates that are downloaded have these package settings and program settings by default. After you click **Save changes**, in a dialog box that appears, you can choose to update existing software update policies and packages. Note that updating existing packages can be time-consuming. If you do not want to update existing packages at this time, you can click **Save only**.

See "Downloading and distributing software updates" on page 46.

Table 5-2 Options on the **Software Update Options** tab of the vendor settings page

Option	Description
Verify authenticity of downloaded Software Updates	Ensures that all software updates are certified. This option is checked by default.
Patch Filter Update Interval	Specifies when to update the target filters for all software updates. By default, the filter update is performed every 30 minutes.
The default Resource Target used by the Software Update Policy Wizard	Specifies the filter that is used by default when you create a new software update policy using the **Distribute Software Updates** wizard. The default target is **Linux Computers with Software Update Plug-in Installed Target**.

Table 5-3 Options on the **Policy and Package Settings** tab of the vendor settings page

Option	Description
Delete packages after	Lets you specify after what time to delete the software update packages that are no longer needed. Default: one week.
Assign package to	Lets you select the package distribution method. For more information on assigning packages to package servers, see the *Symantec Management Platform User Guide*.

Table 5-3 Options on the **Policy and Package Settings** tab of the vendor settings page *(continued)*

Option	Description
Use alternate download location on Package Server	Lets you specify a different location on a package server to which to download packages. This setting accepts the following values: ■ C:\myfolder\ ■ \\myserver\myshare\ ■ \\%computername%\myshare\ In this case, %computername% is a token that will be substituted with a package server computer name. The share must exist on the package server and be accessible with the Agent Connectivity Credentials (ACC). If these conditions are not met, the packages will be marked as invalid. If you are using Linux package servers in your environment, the Windows path that you specify is converted to UNIX paths automatically. You must use the trailing slash for the conversion to work correctly. For example, c:\path\ is converted to /path/ on Linux package servers.
Use alternate download location on client	This option is disabled for Linux computers.

Table 5-4 Options on the **Programs** tab of the vendor settings page

Option	Description
Terminate after	Lets you specify a time after which to terminate a running software update program. Default: two hours.

Table 5-5 Options on the **Novell Customer Center** tab of the vendor settings page

Option	Description
Novell mirror credentials	(**Novell Patch Remediation Settings** policy only) Type the Novell mirror credentials. Patch Management Solution for Linux uses these credentials to download the software updates catalog from the Novell Web site.

Table 5-6 Options on the **Red Hat Network** tab of the vendor settings page

Option	Description
Red Hat Network access credentials	(**Red Hat Patch Remediation Settings** policy only) Type the Red Hat Network credentials. Patch Management Solution for Linux uses these credentials to download the software updates catalog from the Red Hat Web site. All managed computers on the same Notification Server must use the same Red Hat Network account.

Default Software Update Plug-in Settings page

This page lets you specify settings for the software update plug-in to use when you install software updates on managed computers.

By default, the settings that you specify on this page apply to all Linux computers that have the software update plug-in installed.

See "About the software update plug-in" on page 23.

See "Configuring software updates installation settings" on page 29.

Table 5-7 Options on the **Installation Schedules** tab of the **Default Software Update Plug-in Settings** page

Option	Description
Schedule	Lets you configure a schedule when software updates get installed on the managed computer. If maintenance windows are specified in Notification Server configuration policies, this schedule is ignored unless you check **Override maintenance windows settings**.

Table 5-7 Options on the **Installation Schedules** tab of the **Default Software Update Plug-in Settings** page *(continued)*

Option	Description
Reinstallation attempts after task failure	Lets you set the number of times Patch Management Solution should attempt to reinstall a software update if the initial install attempt fails. Default: three times.
Allow user to run	Lets a user initiate software update installation on the target Linux computer by running the `aex-patchinstall -i` command.
Override maintenance windows settings	If maintenance windows are set up for Linux computers, you can install software updates only within maintenance windows. If an update is scheduled to install outside of a maintenance window, it is not installed. Check this option to override this behavior and use the install options that you specified in this policy. Uncheck to abide by the maintenance windows that are specified in Notification Server configuration policies.

Table 5-8 Options on the **Notification** tab of the **Default Software Update Plug-in Settings** page

Options	Description
Notify user	Lets you choose to send a message to the users of the computer on which a patch management task is about to run. Specify for how long the message should be displayed before a task is run. You can type a custom message: for example, “Software updates will install on your computer in 10 minutes. Please ensure that all work is saved”.

Run System Assessment Scan on Linux Computers task

This task lets you run a system assessment scan on the target computers outside of the normal system assessment schedule that is defined on the **System Assessment Scan Settings** page.

See “Configuring the system assessment scan interval ” on page 30.

Chapter 6

Configuring Patch Management Solution server tasks

This chapter includes the following topics:

About Patch Management Solution server tasks

You must configure server tasks (previously known as background actions) to run automatically at regular intervals.

Examples of server tasks include **Import Patch Data for Novell** and **Import Patch Data for Red Hat**. Automated server tasks ensure that you have the latest, most accurate data, and that your software update tasks are kept up-to-date. To configure a task to run automatically, set a schedule for it.

The **Import Patch Data for Novell** and **Import Patch Data for Red Hat** tasks must successfully run before you can download or distribute any software updates for Linux computers.

These tasks download software updates catalog files and import all software management resources from these files into the CMDB.

See "Downloading the software updates catalog" on page 38.

See "Implementing Patch Management Solution for Linux" on page 15.

Other server tasks ensure data integrity or assist in automating software update distribution processes.

See "Relocating or checking the integrity of software update packages" on page 39.

Downloading the software updates catalog

You must download the Novell and Red Hat software updates catalog (patch management metadata, or patch management import files) before you can distribute updates.

See "Implementing Patch Management Solution for Linux" on page 15.

The software updates catalog is downloaded from the following URLs:

- Red Hat — http://xmlrpc.rhn.redhat.com
- Novell — https://nu.novell.com

You need to make sure that your firewall configuration and proxy configuration allow network communication to these URLs.

You may want to create a schedule for this task as well. This procedure ensures that you have the latest, most accurate data, and your software update tasks are kept up-to-date. Symantec recommends that you configure the task to run weekly.

Note: If the Altiris Log Viewer is open, close it before you perform this task. By closing the viewer, you can improve the task's performance by as much as 50 percent.

See "Implementing Patch Management Solution for Linux" on page 15.

To download the software updates catalog immediately

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management**.
3. Click one of the following:
   - **Import Patch Data for Novell**
     This task downloads the Novell patches metadata.
   - **Import Patch Data for Red Hat**
     This task downloads the Red Hat errata metadata.

4 In the right pane, click **Import channels**.

5 When the software channels import is complete, check the channels for which you want to download the patch management metadata.

For Red Hat, check only the base channels (operating system names) for which you want to download the metadata. If you want, you can expand the tree and check any additional components, such as development tools.

For Novell, checking the base channels (operating system names) selects all of the child items in the tree for download. You can reduce the metadata download time by unchecking unnecessary subchannels. However, Symantec recommends that for each of the **Update** channels you also check the respective **Pool** channel. Doing so improves dependency resolving.

6 (Optional) Make any wanted changes.

See "Import Patch Data for Novell and Import Patch Data for Red Hat pages" on page 40.

7 Click **Save changes**.

8 Under **Task Status**, click **New Schedule**.

9 In the **New Schedule** dialog box, click **Now**, and then click **Schedule**.

To configure a schedule for downloading the software updates catalog

1 On the **Import Patch Data for Novell** or **Import Patch Data for Red Hat** page, under **Task Status**, click **New Schedule**.

2 In the **New Schedule** dialog box, click **Schedule**, and then configure a schedule on which to run this task.

Symantec recommends that you configure the task to run weekly.

3 Click **Schedule**.

Relocating or checking the integrity of software update packages

When you change package or program settings in the **Patch Remediation Settings** policies, you can choose to run the **Check Software Update Package Integrity** task. This task checks that all software update packages have the correct new settings and values.

See "Configuring Linux remediation settings" on page 29.

You can also run this task manually to verify that software update packages in software update tasks have the correct global server settings applied.

The task also relocates the software update packages in case you changed the default software update package location on the **Core Services** page.

See "Configuring patch management Core Services settings" on page 27.

To relocate or check the integrity of software update packages

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **System Jobs and Tasks > Software > Patch Management**, and then click **Check Software Update Package Integrity**.
3. If you want to delete the downloaded updates that are not part of any software update policy or belong to a superseded bulletin, check **Delete the updates that are no longer in use from the file system**.
4. If you changed the **Software Update Package Location** value on the **Core Services** page and want to relocate downloaded updates, check **Relocate existing packages if default Software Update package location on Core Services page has changed**.

   See "Configuring patch management Core Services settings" on page 27.
5. Under **Task Status**, click **New Schedule** and specify a schedule on which to run the task.

Import Patch Data for Novell and Import Patch Data for Red Hat pages

This task downloads the software update catalog files and imports all software update resources from these files into the CMDB. These resources are necessary for populating the **Patch Remediation Center** and performing the system assessment scan on the managed computers.

This task downloads the information about the updates that are available for download. It does not download the actual software update files.

See "Downloading the software updates catalog" on page 38.

Table 6-1 Options on the **Import Patch Data** page

Option	Description
Incremental Import	Check to import only the updates that have been added since the last successful import.

Table 6-1 Options on the **Import Patch Data** page *(continued)*

Option	Description
Automatically revise Software Update policies after importing patch data	Automatically updates software update policies with the latest data. Each download of the patch management metadata files may contain data and fixes for the software bulletins that were published earlier. By checking this option, you can use the new data to resolve any known issues with existing software bulletins.
Enable distribution of newly added Software Updates	Enables the distribution of the software updates that were added to existing software bulletins by the software vendor. If you check this option, the software updates that are added to existing software update policies will be enabled for distribution. If you do not check this option, the software updates will be added to the policy, but not enabled.

Table 6-1 Options on the **Import Patch Data** page *(continued)*

Option	Description
Select software channels for import	Lets you choose the operating systems and channels for which you want to import the updates catalog. When you run this task for the first time, you must click **Import channels** to download the list of available software channels. You should check only the operating systems that are installed on the computers that you want to manage. For Red Hat, check only the base channels (operating system names) for which you want to download the metadata. If you want, you can expand the tree and check any additional components, such as development tools. For Novell, checking the base channels (operating system names) selects all of the child items in the tree for download. You can reduce the metadata download time by unchecking unnecessary subchannels. Note that Novell has an overlap period of support for six months after a new service pack is released. After the six-month overlap period, Novell stops publishing new updates for the previous service pack. Novell recommends that you migrate to the latest service pack within this six-month period. However, the computers that have not been migrated can continue receiving updates from Patch Management Solution for Linux. To do this, select a software channel for the latest available service pack. Some updates from this channel can also be applied to the Novell systems with a lower service pack version. For more information, see the end of life announcements on the Novell Web site.

Chapter 7

Downloading and distributing software updates

This chapter includes the following topics:

About errata and patches

Software bulletins that contain security updates for Red Hat Linux servers are called errata. Periodically, Red Hat issues the Red Hat Security Advisories (RHSA), Red Hat Bug Advisories (RHBA), and Red Hat Enhancement Advisories (RHEA),

which are the equivalent of Microsoft software bulletins. The advisories are either security fixes, bug fixes, or enhancements. Each advisory contains one or more patches (rpm packages). All the RHSAs, RHBAs, and RHEAs are available at the following URL: https://rhn.redhat.com/errata.

Software bulletins that contain SUSE security updates for Novell Linux servers are called patches. Novell patches for different products may be released several times in a month.

See "About downloading and distributing software updates" on page 44.

About downloading and distributing software updates

You can download errata or patches on the **Patch Remediation Center** page, where all available software updates are listed. You can also do this from any Patch Management Solution report.

See "About errata and patches" on page 43.

When you choose to download an erratum or patch, all associated updates are downloaded to the Notification Server computer.

You can choose to download the software update packages now but distribute them at a later time. You also have an option to download and distribute the software update to managed computers at once.

When in the **All Software Bulletins** report, the value in the **Staged** column changes to **True**, all updates for the erratum or patch have been downloaded.

See "Downloading software updates" on page 44.

To reduce workload on the Notification Server computer, Symantec recommends that you create software update policies in monthly increments. Including a large number of errata or patches into a software update policy can affect performance and make managing updates difficult.

See "Downloading and distributing software updates" on page 46.

Warning: Patch Management Solution for Linux does not support the rollout of kernel updates because the automatic restart functionality is not available. Do not stage and distribute kernel updates.

Downloading software updates

You can download an erratum or patch and its associated updates.

You can download all errata or patches. However, Symantec recommends that you download only the errata or patches that the target computers require. On the **Patch Remediation Center** page, in the compliance reports, you can view how many computers require an update.

After the updates are downloaded, you must create a software update policy to distribute the updates to managed computers.

See "Downloading and distributing software updates" on page 46.

When you choose to download an erratum or patch, a task is created that downloads the software updates. You can view the status of this task to troubleshoot the download of software updates.

See "About downloading and distributing software updates" on page 44.

See "Implementing Patch Management Solution for Linux" on page 15.

To download software updates

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down list, click **Red Hat Compliance by Erratum** or **SUSE Compliance by Announcement**, and then click the **Refresh** symbol.

   These reports let you see which updates the target computers require.
3. Click the errata or patches that you want to download.

   For example, click the errata or patches that have a lower number in the **Compliance** column. You can select multiple items while holding down the Shift or Control key.
4. Right-click the selected errata or patches, and then click **Download packages**.

   You can close the status dialog box and the download continues in the background.

To view the status of a software updates download

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management**, and then click **Download Software Update Package**.
3. In the right pane, view the status of download tasks.

Downloading and distributing software updates

To deliver and install the software updates to the appropriate computers, you must create software update policies.

The **Distribute Software Updates** wizard lets you create software update policies. If the associated software updates are not yet downloaded, Patch Management Solution creates a download task. When download is completed, the software update policy is distributed to the target computers.

To reduce workload on the Notification Server computer, Symantec recommends that you create software update policies in monthly increments. Including a large number of errata or patches into a software update policy can affect performance and make managing updates difficult.

The policies that you create are stored in the **Manage > Policies > Software > Patch Management > Software Update Policies** folder. You can view the details of the policy and change settings if necessary.

You can view the software update policies distribution results in reports.

See "Viewing the software update delivery summary report" on page 47.

Warning: Patch Management Solution for Linux does not support the rollout of kernel updates. Do not distribute kernel updates.

See "About downloading and distributing software updates" on page 44.

See "Implementing Patch Management Solution for Linux" on page 15.

To distribute software updates

1. In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**.
2. In the right pane, in the **Show** drop-down box, click **SUSE Compliance by Announcement** or **Red Hat Compliance by Errata**, and then click the **Refresh** symbol.

   These reports let you see which updates the target computers require.
3. Click the errata or patches that you want to distribute.

   For example, click the errata or patches that have a lower number in the **Compliance** column. You can select multiple items while holding down the Shift or Control key.
4. Right-click the selected bulletins, and then click **Distribute Packages**.

5 (Optional) Configure the settings as needed.

See "Distribute Software Updates wizard pages" on page 50.

6 Click **Next**.

7 (Optional) On the second page of the wizard, check the updates that you want to distribute.

8 If you want to activate the new software update policy, turn on the policy. To turn on the policy, click the colored circle and then click **On**.

You can also turn on the policy later.

9 Click **Distribute software updates**.

Viewing the software update delivery summary report

The **Linux Software Update Tasks Delivery Summary** report summarizes the results of all scheduled software update policies. It tells you which computers the software update tasks target, and if the updates have been successfully installed. The report also tells you if any software update tasks failed, or if they have not yet completed.

Patch Management Solution for Linux also provides other reports that you can view.

See "About Patch Management Solution reports" on page 55.

See "Implementing Patch Management Solution for Linux" on page 15.

To view the software update delivery summary report

1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2 In the left pane, expand **Software > Patch Management > Remediation Status**, and then click **Linux Software Update Tasks Delivery Summary**.

3 In the right pane, leave the default settings, and then click **Refresh**.

About software update policies and maintenance windows

Maintenance windows are time periods in which installation of software updates and other maintenance tasks are performed. To ensure that software update policies abide by maintenance windows, leave the **Override Maintenance Window Settings** check box unchecked on the first page of the **Distribute Software Updates** wizard.

On Linux computers, software updates can be installed only at the scheduled time. Make sure that you schedule the updates installation within the maintenance window.

If you check the box, the software update plug-in ignores maintenance windows and installs the updates as instructed by the software update policy.

See "Distribute Software Updates wizard pages" on page 50.

Installing a software update may take longer than a specified maintenance window. In this case, the installation of the updates completes, but any required restarts are deferred until the next maintenance window.

Patch Remediation Center page

This page lets you view, download, and distribute the software updates that the software update metadata files provide.

See "About downloading and distributing software updates" on page 44.

See "About errata and patches" on page 43.

Table 7-1 Items on the **Patch Remediation Center** page

Item	Description
Bulletin	The bulletin's number, as supplied by the vendor.
Severity	The bulletin's vendor-specified severity level.
Custom Severity	The bulletin's user-defined severity level.
Staged	The download status of the software updates for this bulletin. If all updates have been downloaded, the result is **True**. Otherwise it is **False**.
Policies	The number of software update policies that have been created from the bulletin.
Updates	The number of software updates that are included in the bulletin.
Downloaded	The number of software updates currently downloaded.
Released	The date the bulletin was released.
Revised	The date the bulletin was revised.
Description	A description of the vulnerabilities that the software bulletin addresses.

Table 7-2 Right-click actions in the **All Software Bulletins** report

Item	Description
Resource Manager	Opens the **Resource Manager** for the selected bulletin. For more information, see the *Symantec Management Platform User Guide*.
Export	Lets you export the bulletin information to an XML file.
Properties	Displays the item's properties and audit information.
CMDB Functions	This option is displayed when Altiris CMDB Solution is installed. For more information, see the *CMDB Solution User Guide*.
Custom Severity	Lets you assign a custom severity level. See "Creating and assigning custom severity levels" on page 28.
Add To Filter	This option is displayed when Altiris CMDB Solution is installed. For more information, see the *CMDB Solution User Guide*.
Add to organizational group	Lets you add a resource to an organizational group.
Disable	Lets you disable the distribution of the bulletin. If the bulletin is already included in a software update policy, it will not be installed. To enable the bulletin, use the **Download Packages** or **Recreate Packages** commands.
Distribute Packages	Launches the **Distribute Software Updates** wizard.
Download Packages	Initiates the download of software update packages. This option is not available if the packages are already downloaded.
Recreate Packages	Lets you check the integrity of downloaded packages and re-download if necessary. This option is not available if the packages are not yet downloaded.

Table 7-2 Right-click actions in the **All Software Bulletins** report *(continued)*

Item	Description
View Policies	Lets you view the software update policies that contain this particular bulletin. This option is available only if a policy has been created for this bulletin.
View Targeted Computers	Displays the computers that the software update policy containing this bulletin is targeting. You must create a software update policy before you can view targeted computers. The bulletin must not be disabled.
List Software Updates	Displays the list of software updates that are included into the software bulletin.

Table 7-3 Right-click actions in the **Windows Compliance by Bulletin** report

Item	Description
View Software Bulletin Information	Displays the software bulletin information such as description, release date, applicable operating systems, and so on.
View Targeted Computers by Bulletin	Displays the computers that the software update policy containing this bulletin is targeting. You must create a software update policy before you can view targeted computers. The bulletin must not be disabled.
View Applicable Computers by Bulletin	Displays the computers to which the selected bulletin applies.
View Installed Computers by Bulletin	Displays the computers on which the selected bulletin is installed.
View Not Installed Computers by Bulletin	Displays the computers that do not have the selected bulletin installed.

Distribute Software Updates wizard pages

The **Distribute Software Updates** wizard creates the software update policies that distribute software updates to managed computers. A software update policy that is created from an erratum or patch includes every software update that is

associated with the erratum or patch. If needed, a download task is created that downloads software update packages from the vendor.

See "Downloading and distributing software updates" on page 46.

Table 7-4 Options on the first page of the **Distribute Software Updates** wizard

Option	Description
Name	The name of the software update policy that you want to create. This field is populated automatically with the bulletin names.
Description	The description of the software update policy that you want to create. This field is populated with the vendor description of the selected bulletins.
Software Bulletins	The names of the bulletins for which you have chosen to make policies. You can click a software bulletin to open the Resource Manager to view detailed information on the software bulletin. You cannot edit the software bulletins through the **Distribute Software Updates** wizard.
Software Updates	The names of each software update that is included in the bulletin.
Run (other than agent default)	Runs the software updates installation at a different time than the time that is specified in the software update plug-in settings. See "Configuring software updates installation settings" on page 29.
As soon as possible	Runs the software updates installation as soon as the software update policy arrives to the target computer.
On schedule	Runs the software updates installation on a schedule.
Override Maintenance Windows settings	Overrides the specified maintenance windows settings. See "About software update policies and maintenance windows" on page 47.

Table 7-4 Options on the first page of the **Distribute Software Updates** wizard *(continued)*

Option	Description
Apply to computers	Lets you specify the target collection or collections to which the software update policy applies. If you use the **Distribute Software Updates** wizard, the correct resource target for the selected software bulletin is automatically applied.

Table 7-5 Options on second page of the **Software Update Policy Wizard**

Options	Description
On/Off	Lets you enable or disable the software update policy for the software bulletin and included software updates. Click **On** if you want the policy to become active after you complete the wizard. You can also turn on the policy later. The policies that you create are located at **Manage > Policies > Software > Patch Management > Software Update Policies**.
Immediately replicate that policy down the hierarchy	This option is available only on the parent Notification Server computer in a hierarchy. Lets you replicate the software update policy immediately down the hierarchy bypassing the default replication schedules. Use this option to replicate an emergency software update. Keep in mind that software update installation is not performed immediately after you create and replicate a software update policy. Software update installation time depends on the software update policy, solution, and the Symantec Management Agent settings.
Software Bulletins	The names of the software bulletins that are included into the software update policy.
Update Names	The name of each software update executable. If you enable this advertisement, all of the executables are enabled. Click the hyperlink to open the **Resource Manager** page for the software update.

Update download and policy creation status dialog

This dialog box displays the package download or software update policy creation status.

You can close this dialog box. The action will continue to run in background.

See "About downloading and distributing software updates" on page 44.

Distribute Software Updates task

Patch Management Solution uses this task to distribute software updates. This task uses the Symantec Management Agent's built-in software management framework functionality to distribute and install updates.

See "About downloading and distributing software updates" on page 44.

This task is read-only.

Download Software Update Package task

Patch Management Solution uses this task to download software updates from the vendor to a local repository.

See "About downloading and distributing software updates" on page 44.

This task is read-only.

Chapter 8

Using Patch Management Solution reports

This chapter includes the following topics:

About Patch Management Solution reports

You can view and manage your patch management data through reports. Reports give you the information that is specific to Patch Management Solution. For example, you can use compliance reports to determine how many urgent software updates your managed computers require.

See "About compliance reports" on page 56.

Reports let you view information in various ways. You can see your information in tables or graphically in charts. You can also drill down on specific items in a report to obtain additional information.

You can download or distribute software updates directly from reports by right-clicking the update name in the report.

Patch Management Solution provides the following reports:

- Compliance reports
  See "About compliance reports" on page 56.
- Diagnostic reports
  See "About diagnostics reports" on page 57.
- Remediation status reports
  See "About remediation status reports" on page 57.
- Software bulletin reports
  See "About software bulletins reports" on page 57.

See "Viewing Patch Management Solution reports" on page 58.

Patch Management Solution also has a patch management portal page that is comprised of a number of Web parts displaying results from commonly used reports.

See "About the Linux compliance dashboard" on page 57.

About compliance reports

Compliance reports let you quickly determine which software updates your managed computers require. Compliance reports are used to determine if computers are up-to-date with the latest software updates. These reports are also used to check if a particular software bulletin or update is installed on your managed computers. This capability is useful if a specific security issue affects your network environment and a certain update addresses the problem.

You can start distributing software updates directly from report results. For example, if you want to quickly distribute all critical updates, sort the report results by **Severity**. Then, right-click all critical updates and click **Download Packages** or **Distribute Packages**.

See "About downloading and distributing software updates" on page 44.

You can find the compliance reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Compliance**.

Compliance reports are also featured on the Patch Management Solution compliance dashboard for easy access.

See "About the Linux compliance dashboard" on page 57.

See "About Patch Management Solution reports" on page 55.

About diagnostics reports

The diagnostics reports display vulnerability summary and software update plug-in installation information.

You can find the diagnostics reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Diagnostics**.

See "About Patch Management Solution reports" on page 55.

About remediation status reports

The remediation status reports summarize and detail software update associations and activities.

You can find the remediation status reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Remediation Status**.

See "About Patch Management Solution reports" on page 55.

About software bulletins reports

The software bulletins reports summarize and detail software bulletins activity and status.

You can find the software bulletins reports in the Symantec Management Console under **Reports > All Reports > Software > Patch Management > Software Bulletins**.

See "About Patch Management Solution reports" on page 55.

About the Linux compliance dashboard

The **Red Hat Software Update Compliance Portal** and **Novell Software Update Compliance Portal** pages provide patch management summary information at a glance. The pages are comprised of a number of Web parts displaying results from commonly used reports.

See "About Patch Management Solution reports" on page 55.

You cannot customize this portal page directly. If you want, you can add patch management Web parts to other configurable portal pages. For example, the **My Portal** page.

You can access the portal page by clicking **Home > Patch Management**, and then, in the left pane, under **Novell** or under **Red Hat Linux**, click **Compliance Dashboard**.

Table 8-1 Web parts on the **Software Update Compliance Portal** pages

Web part	Description
Patch Management License Status	Reports on the amount of Patch Management Solution licenses in use, their status, and expiration date.
Vulnerabilities	Reports on the number of vulnerabilities that need to be addressed. This Web part is also available in a graph form.
Software Update Tasks Delivery Summary	Reports on the number of patches that were executed in the past 30 days and how many succeeded or did not complete. This Web part is also available in a graph form.
Software Bulletin Summary	Reports on the number of software bulletins available, staged, tasks created, and new bulletins in the last 30 days. This Web part is also available in a graph form.
Configuration Summary	Provides an overall configuration summary, which includes computers with the software update plug-in, computers not reporting vulnerability analysis, software updates catalog download data, and so on.

Viewing Patch Management Solution reports

Patch Management Solution for Windows provides reports that let you view detailed information about the updates.

See "About Patch Management Solution reports" on page 55.

To view Patch Management reports

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Software > Patch Management**.
3. Click the report that you want to view.

   For example, click **Compliance > SUSE Compliance by Update**.

4 In the right pane, leave the default settings, and click **Refresh**.

5 If you want to view more information about an update, right-click any update, and click **Resource Manager**.

Chapter 9

Replicating Patch Management Solution for Linux data in hierarchy

This chapter includes the following topics:

About replicating Patch Management Solution for Linux data in hierarchy

Downloading Red Hat and Novell patch management metadata files to multiple Notification Server computers can consume considerable network resources and time. Notification Server hierarchy features remove the need to download patch management metadata files individually. You can download the files once to a single parent Notification Server computer. Then you can use Patch Management Solution replication rules to send the relevant data to any number of child Notification Server computers. The replicated data on the child Notification Server computers is identical to the data on the parent.

Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another child.

Replication is possible as soon as you install the software update plug-in on the child Notification Server computer's Linux client computers. The software update plug-in collects operating system inventory data that is then sent to the parent Notification Server computer by the **Patch Linux OS Channel Resource Replication Rule**. If the clients that match the selected software channels exist on the child Notification Server computer, patch management metadata files can

be replicated to that server. By default, the operating system inventory data is replicated once a day at 20:00.

To enable Red Hat and Novell patch management metadata files replication, you must turn on the **Patch Management Import Data Replication for Novell** and **Patch Management Import Data Replication for Red Hat** rules on the parent Notification Server computer. When the rules are turned on, replication is performed once a day at 23:00.

See "About Patch Management Solution for Linux" on page 11.

Appendix A

Technical reference

This appendix includes the following topics:

About hierarchy and data replication direction

Patch Management Solution for Windows and Patch Management Solution for Linux support the hierarchy and the replication features of the Symantec Management Platform. These features let you create settings, schedules, and other data at the top-level Notification Server computer and replicate them to child-level Notification Server computers.

Patch Management Solution for Mac does not support replication.

See "About replicating Patch Management Solution for Linux data in hierarchy" on page 61.

Table A-1 Items that are replicated by the default Notification Server replication schedule with no custom replication rules

Item	Replication direction
All the server tasks settings and schedules: ■ **Check Software Update Package Integrity** ■ **Import Patch Data for Windows/Red Hat/Novell**	Down
Run System Assessment Scan on Windows/Linux Computers task settings and schedules	Down
Windows/Linux System Assessment Scan policy settings	Down
Windows/Red Hat/Novell Patch Remediation Settings policy	Down

Table A-1 Items that are replicated by the default Notification Server replication schedule with no custom replication rules *(continued)*

Item	Replication direction
Default Software Update Plug-in Policy settings	Down
Software update plug-in install, upgrade, and uninstall policy settings	Down
Software update policies	Down

Table A-2 Items that are replicated with custom replication rules

Item	Replication direction	Description
Language support information (Patch for Windows only)	Up	This information is replicated when the **Patch Management Language Alerting** rule is enabled.
OS inventory data (Patch for Linux only)	Up	This information is replicated when the **Patch Linux OS Channel Resource Replication Rule** is enabled.
Patch management metadata	Down	This information is replicated when the **Patch Management Import Data Replication for Windows/Red Hat/Novell** rules are enabled. For Windows, only the updates and bulletins that are associated with the child computer's supported languages are replicated. For Linux, only the metadata for the channels that are relevant to the child Notification Server's client computers is replicated.
Compliance summary	Up	This information is replicated when the **Patch Compliance Summary Replication** rule is enabled. The system assessment scan result is replicated up as a summary.

About Patch Management Solution security roles

You can assign the following security roles to Symantec Management Console users:

- **Patch Management Administrators**
- **Patch Management Rollout**

Users with the **Patch Management Administrators** role have full access to Patch Management Solution functionality, but no access to the rest of the Symantec Management Console.

Users with the **Patch Management Rollout** role have limited access to the following Patch Management Solution functionality:

- Software update policies
- Reports
- Patch Remediation Center page

Users with the **Patch Management Rollout** role can perform the following actions:

- Enable, disable, and change settings in the software update policies.
- View reports.

Appendix B

Altiris™ Patch Management Solution for Linux 7.1 SP2 from Symantec™ Third-Party Legal Notices

This appendix includes the following topics:

Third-Party Legal Attributions

This Symantec product may contain third party software for which Symantec is required to provide attribution (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. This appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

XML-RPC.NET

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder" in the license below means the copyright holder listed above.

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Index

P

R

S

U

V